UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/658,310	09/09/2003	Ed H. Frank	14177US02	2145

23446 7590 11/12/2008

MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
11/12/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/658,310	FRANK ET AL.	
	Examiner	Art Unit	
	CARLTON V. JOHNSON	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 July 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Pre-Appeal Request filed on 7-25-2008, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

2. Claims **1 - 42** are pending. Claims **1, 15, 29** have been amended. Claims **1, 15, 29** are independent. This application was filed on **9-9-2003**.

Response to Arguments

3. Applicant's arguments filed 7-25-2008 have been fully considered and they were persuasive therefore new grounds of rejection has been entered.

Response to Arguments:

The Weatherspoon prior art discloses a first channel for authentication initiation (request). (see Weatherspoon col. 4, lines 23-29: plurality of APs and corresponding devices; col. 4, lines 32-37: establishes a communications channel)

And, the Weatherspoon prior art discloses a second channel for authentication information. (see Weatherspoon col. 5, lines 12-19: if the wireless device is valid the AP establishes a control channel with the authentication server; transmits encrypted authentication messages that includes operator's logon name and password)

In addition, the Weatherspoon prior art discloses a third channel for hosting (data transfers) a communications session. (see Weatherspoon col. 5, lines 29-37:

authentication server validates both the AP and operator, authentication server will enable access to the wired LAN)

The Chandrashekhar prior art discloses a communications link between two network nodes to request the initiation and setup of a communications session. Chandrashekhar discloses a communications link between two network nodes to perform an authentication procedure. And, the Chandrashekhar prior art discloses a communications link between two network nodes for the transmission and receipt of communications data (a session). In addition, the Chandrashekhar prior art discloses communications completed over a wireless communications network using access points. (see Chandrashekhar paragraph [0112], lines 1-5; paragraph [0112], lines 27-28)

The Chandrashekhar prior art discloses an authentication procedure over network communications. The Chandrashekhar prior art discloses authentication using a first physical (PHY) channel for a request for VPN service and a second physical (PHY) channel for the authentication procedure. (see Chandrashekhar Figure 3; paragraph [0057], lines 1-5; paragraph [0062], lines 1-4) The VPN manager utilizes an authentication server, which is connected by a communications bus or communications path and performs the authentication procedure. This is a different communications path than utilized for the request for VPN service from user1 to the VPN manager (enhanced application portal). The Chandrashekhar prior art discloses the claim limitation of a first channel for processing a request and a second channel for

authentication.

The successful responses to arguments for independent claims 1, 15, 29, also successfully respond to the current arguments against the dependent claims 6-9, 12-14, 20-23, 26-28, 34-37 and 40-42.

Each obviousness combination indicates the claim limitation the combined prior art references teaches. In addition, a cited passage from the referenced prior art indicates the motivation for the obviousness combination. Each obviousness combination's disclosure is equivalent to Applicant's claim limitation(s) for the claimed invention.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims **1, 6 - 9, 12 - 15, 20 - 23, 26 - 29, 34 - 37, 40 - 42** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Chandrashekhar et al.** (US PGPUB No. **20030140131**) in view of **Giniger et al.** (US Patent No. **6,751,729**) and further in view of **Weatherspoon et al.** (US Patent No. **7,174,564**).

With Regards to Claims 1, 15, 29, Chandrashekhar discloses a method, machine-

readable storage having stored upon a computer program having at least one code section, system for multiple encryption in a multi-band multi-protocol hybrid wired/wireless network, the method comprising: receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device; authenticating said communication session by authenticating said access using a second PHY channel; and hosting said communication session over a third PHY channel , said third PHY channel established between said access point and said originating access device. (see Chandrashekhar paragraph [0054], lines 3-5; paragraph [0054], lines 10-12: hybrid communications network; paragraph [0040], lines 4-6; paragraph [0108], lines 1-5: wireless/wired communications; paragraph [0056], lines 1-3: request for communications service; paragraph [0048], lines 1-7: software, implementation means); Figure 3; paragraph [0112], lines 1-5; paragraph [0112], lines 27-28: access point communications device(s)) Chandrashekhar does not specifically disclose whereby authenticating said originating access device. However, Giniger discloses wherein authenticating said originating access device. (see Giniger col. 3, lines 21-25: VPN (tunnel) communications; col. 4, lines 59-67; col. 5, lines 6-10; col. 15, lines 27-33: authentication, network device)

It would have been obvious to one of ordinary skill in the art to modify Chandrashekhar to authenticate a network device (an originating access device) as taught by Giniger. One of ordinary skill in the art would have been motivated to employ the teachings of Giniger in order for the selection of the optimum path based on security policy, setup conditions and routing parameters to optimized bandwidth, save time, and

reduce operating costs. (see Giniger col. 6, lines 31-38: "*... Dynamic routing enables the creation of meshed VPN network topologies. The optimum path is automatically selected based on security policy, setup connections, and routing parameters to optimize bandwidth, save time, and reduce operating costs. On a larger scale, users can form communities of interest by creating their own virtual networks within existing enterprise topologies using private or public networks. ...* ")

In addition, Weatherspoon discloses wherein a method, machine-readable storage having stored upon a computer program having at least one code section, system for multiple encryption in a multi-band multi-protocol hybrid wired/wireless network, the method comprising: receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device (see Weatherspoon col. 4, lines 23-29: plurality of APs and corresponding devices; col. 4, lines 32-37: establishes a communications channel); authenticating said communication session by authenticating said access using a second PHY channel (see Weatherspoon col. 5, lines 12-19: if the wireless device is valid the AP establishes a control channel with the authentication server; transmits encrypted authentication messages that includes operator's logon name and password); and hosting said communication session over a third PHY channel, said third PHY channel established between said access point and said originating access device. (see Weatherspoon col. 5, lines 29-37: authentication server will enable access to the wired LAN by establishing a data channel between the AP and any other device on the wired LAN)

It would have been obvious to one of ordinary skill in the art to modify Chandrashekhar to enable a first, second, and third communications channel for authentication and data transfers as taught by Weatherspoon. One of ordinary skill in the art would have been motivated to employ the teachings of Weatherspoon in order for a secure wireless local area network that is inexpensive, easy to set up, fast, and reliable. (see Weatherspoon col. 3, lines 9-11: " *... Accordingly, a need remains for a secure wireless local area network that is inexpensive, easy to set up, fast, and reliable....* ")

With Regards to Claims 6, 20, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 1, 15, comprising receiving an identification of said originating access device by said access point. (see Chandrashekhar paragraph [0073], lines 13-16: identification for originating device, user; paragraph [0037], lines 4-15: access network (i.e. access point))

With Regards to Claims 7, 21, 35, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having one code section, system according to claims 6, 20, 34, wherein said identity of said originating access device is one or more of a WEP key, a MAC address, and/or an IP address. (see Chandrashekhar paragraph [0073], lines 13-16; paragraph [0082], lines 14-16: IP address utilized as identification)

With Regards to Claims 8, 22, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 1, 15, comprising acknowledging said received request on said first PHY channel. (see Chandrashekhar paragraph [0057], lines 3-7: response to received request (i.e. response, ACK))

With Regards to Claims 9, 23, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 1, 15, comprising determining a type of traffic generated by said originating access device on said first PHY channel. (see Chandrashekhar paragraph [0028], lines 13-15: type of traffic, VPN; paragraph [0054], lines 7-12: between communications endpoints)

With Regards to Claims 12, 26, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 1, 15, further comprising establishing at least one virtual channel between said originating access device and a terminating access device. (see Chandrashekhar paragraph [0054], lines 7-12: establish circuit between originating device and terminating device (i.e. endpoints, communications circuit); paragraph [0040], lines 4-6: dial-up user, physical circuit))

With Regards to Claims 13, 27, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 12, 26, comprises tunneling information between said originating access device and said terminating access device. (see Chandrashekhar paragraph [0032], lines 2-5; paragraph [0054], lines 7-12; paragraph [0081], lines 7-9: tunneling between originating and termination devices (i.e. endpoints))

With Regards to Claims 14, 28, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 12, 26, comprising establishing at least a portion of said at least one virtual channel over at least a portion of one of said first PHY channel, said second PHY channel or said third PHY channel. (see Chandrashekhar paragraph [0028], lines 13-15; paragraph [0054], lines 7-12: virtual channel between originating and terminating devices (i.e. VPN tunnel, virtual channel endpoints))

With Regards to Claim 34, Chandrashekhar discloses the system according to claim 29, wherein said at least one receiver is adapted to receive an identification of said originating access device by said access point. (see Chandrashekhar paragraph [0073], lines 13-16: identification for originating device, user; paragraph [0037], lines 4-15: access network (i.e. access point))

With Regards to Claim 36, Chandrashekhar discloses the system according to claim

29, wherein said at least one receiver is adapted to acknowledge said received request on said first PHY channel. (see Chandrashekhar paragraph [0057], lines 3-7: response to received request (i.e. response, ACK))

With Regards to Claim 37, Chandrashekhar discloses the system according to claim 29, wherein said at least one authenticator is adapted to determine a type of traffic generated by said originating access device on said first PHY channel. (see Chandrashekhar paragraph [0028], lines 13-15: type of traffic, VPN; paragraph [0054], lines 7-12: between communications endpoints)

With Regards to Claim 40, Chandrashekhar discloses the system according to claim 29, wherein at least one receiver is adapted to establish at least one virtual channel between said originating access device and a terminating access device. (see Chandrashekhar paragraph [0054], lines 7-12: establish circuit between originating device and terminating device (i.e. endpoints, communications circuit); paragraph [0040], lines 4-6: dial-up user, physical circuit))

With Regards to Claim 41, Chandrashekhar discloses the system according to claim 40, wherein said at least one receiver is adapted to tunnel information between said originating access device and said terminating access device. (see Chandrashekhar paragraph [0032], lines 2-5; paragraph [0054], lines 7-12; paragraph [0081], lines 7-9: tunneling between originating and termination devices (i.e. endpoints))

With Regards to Claim 42, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section, system according to claims 40, wherein said at least one receiver is adapted to establish at least a portion of said at least one virtual channel over at least a portion of one of said first PHY channel, said second PHY channel and/or said third PHY channel. (see Chandrashekhar paragraph [0028], lines 13-15; paragraph [0054], lines 7-12: virtual channel between originating and terminating devices (i.e. VPN tunnel, virtual channel endpoints))

6. Claims **2 - 5, 10, 11, 16 - 19, 24, 25, 30 - 33, 38, 39** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Chandrashekhar-Giniger-Weatherspoon** and further in view of **He et al.** (US Patent No. **6,088,451**).

With Regards to Claims 2, 16, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 1, 15. (see Chandrashekhar paragraph [0054], lines 7-12; paragraph [0081], lines 7-9: communications between endpoints; paragraph [0048], lines 1-7: software, implementation means) Chandrashekhar does not specifically disclose generating at least one encryption/decryption key. However, He discloses wherein further comprising generating at least one encryption/decryption key for use during said communication session. (see He col. 18, lines 2-5; col. 19, lines 8-11; col.

20, lines 57-61: generation encryption/decryption key)

It would have been obvious to one of ordinary skill in the art to modify Chandrashekhar for the generation of an encryption/decryption key as taught by He. One of ordinary skill in the art would have been motivated to employ the teachings of He in order for a network-wide centralized user administration and authentication, credential management and network element access. (see He col.1, lines 59-63: *"... It also supports the implementation of network-wide centralized user administration and management, authentication, credential/privilege control and access to individual network elements, which is highly desirable for a large and complex network. ..."*)

With Regards to Claims 3, 17, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 2, 17, wherein said authenticating comprises requesting authentication information from an authentication server. (see Chandrashekhar paragraph [0041], lines 1-5; paragraph [0057], lines 1-3: utilizing an authentication server for authorization)

With Regards to Claims 4, 18, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 3, 17, wherein said authenticating comprises delivering at least a portion of said authentication information received from said authentication server to said originating access device via said second PHY channel. (see

Chandrashekhar paragraph [0057], lines 3-7: appropriate indication returned to user)

With Regards to Claims 5, 19, 33, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section, system according to claims 4, 18, 32. (see Chandrashekhar paragraph [0054], lines 7-12; paragraph [0081], lines 7-9: communications between endpoints) Chandrashekhar does not specifically disclose delivering said encryption/decryption key. However, He discloses wherein comprising delivering said at least one encryption/decryption key to said originating access device via one of said first PHY channel or said second PHY channel. (see He col. 18, lines 2-5; col. 19, lines 8-11; col. 20, lines 57-61: delivering encryption/decryption key; Figure 3)

It would have been obvious to one of ordinary skill in the art to modify Chandrashekhar for delivery of an encryption/decryption key as taught by He. One of ordinary skill in the art would have been motivated to employ the teachings of He in order to a network-wide centralized user administration and authentication, credential management and network element access. (see He col.1, lines 59-63)

With Regards to Claims 10, 24, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 9, 23, further comprising at least one key dependent on said determined traffic type. (see Chandrashekhar paragraph [0054], lines 7-12; paragraph [0081], lines 7-9: communications between endpoints; paragraph [0028], lines 13-15:

virtual channel between originating and terminating device (i.e. VPN tunnel, virtual channel endpoints): key utilized for VPN type traffic, encryption key parameter) Chandrashekhar does not specifically disclose generating at least one encryption/decryption key. However, He discloses wherein comprising generating at least one encryption/decryption key. (see He col. 18, lines 2-5; col. 19, lines 8-11; col. 20, lines 57-61: generation encryption/decryption key)

It would have been obvious to one of ordinary skill in the art to modify Chandrashekhar for generation of an encryption/decryption key as taught by He. One of ordinary skill in the art would have been motivated to employ the teachings of He in order to a network-wide centralized user administration and authentication, credential management and network element access. (see He col.1, lines 59-63)

With Regards to Claims 11, 25, 39, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section, system according to claims 10, 24, 38. (see Chandrashekhar paragraph [0054], lines 7-12; paragraph [0081], lines 7-9: communications between endpoints) Chandrashekhar does not specifically disclose the distribution of generated encryption/decryption key. However, He discloses wherein comprising distributing said generated at least one encryption/decryption key via at one or both of said second PHY channel and/or said third PHY channel. (see He col. 18, lines 2-5; col. 19, lines 8-11; col. 20, lines 57-61: delivering (i.e. distributing) generated encryption/decryption key; Figure 3)

It would have been obvious to one of ordinary skill in the art to modify Chandrashekhar for generation of an encryption/decryption key as taught by He. One of ordinary skill in the art would have been motivated to employ the teachings of He in order to a network-wide centralized user administration and authentication, credential management and network element access. (see He col.1, lines 59-63)

With Regards to Claim 30, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section, system according to claim 29. (see Chandrashekhar paragraph [0054], lines 7-12; paragraph [0081], lines 7-9: communications between endpoints; paragraph [0048], lines 1-7: software, implementation means) Chandrashekhar does not specifically disclose generating at least one encryption/decryption key. However, He discloses wherein further comprising generating at least one encryption/decryption key for use during said communication session. (see He col. 18, lines 2-5; col. 19, lines 8-11; col. 20, lines 57-61: generation encryption/decryption key)

It would have been obvious to one of ordinary skill in the art to modify Chandrashekhar for generation of an encryption/decryption key as taught by He. One of ordinary skill in the art would have been motivated to employ the teachings of He in order to a network-wide centralized user administration and authentication, credential management and network element access. (see He col.1, lines 59-63)

With Regards to Claim 31, Chandrashekhar discloses the system according to claim

30, wherein said at least one authenticator is adapted to request authentication information. (see Chandrashekhar paragraph [0041], lines 1-5; paragraph [0057], lines 1-3: utilizing an authentication server for authorization)

With Regards to Claim 32, Chandrashekhar discloses the system according to claim 31, wherein said authenticator is adapted to deliver at least a portion of said authentication information received from said authentication server to said originating access device via said second PHY channel. (see Chandrashekhar paragraph [0057], lines 3-7: appropriate indication returned to user)

With Regards to Claim 38, Chandrashekhar discloses the system according to claims 37, wherein said at least one authenticator is adapted further comprising at least one key dependent on said determined traffic type. (see Chandrashekhar paragraph [0054], lines 7-12; paragraph [0081], lines 7-9: communications between endpoints; paragraph [0028], lines 13-15: virtual channel between originating and terminating device (i.e. VPN tunnel, virtual channel endpoints): key utilized for VPN type traffic, encryption key parameter) Chandrashekhar does not specifically disclose generating at least one encryption/decryption key. However, He discloses wherein said at least one authenticator is adapted to generate at least one encryption/decryption key. (see He col. 18, lines 2-5; col. 19, lines 8-11; col. 20, lines 57-61: generation encryption/decryption key)

It would have been obvious to one of ordinary skill in the art to modify

Chandrashekhar for generation of an encryption/decryption key as taught by He. One of ordinary skill in the art would have been motivated to employ the teachings of He in order to a network-wide centralized user administration and authentication, credential management and network element access. (see He col.1, lines 59-63)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
October 27, 2008